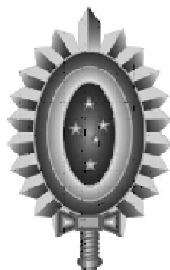
EB70-MC-10.232



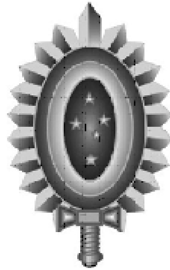
MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COMANDO DE OPERAÇÕES TERRESTRES

Manual de Campanha

GUERRA CIBERNÉTICA

1ª Edição
2017

EB70-MC-10.232



MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COMANDO DE OPERAÇÕES TERRESTRES

Manual de Campanha

GUERRA CIBERNÉTICA

1ª Edição
2017

PORTARIA Nº 42 - COTER, DE 8 DE JUNHO DE 2017

Aprova o Manual de Campanha EB70-MC-10.232
Guerra Cibernética, 1ª Edição, 2017

O COMANDANTE DE OPERAÇÕES TERRESTRES, no uso da atribuição que lhe confere o inciso III do art. 11 do REGULAMENTO DO COMANDO DE OPERAÇÕES TERRESTRES (EB10-R-06.001), aprovado pela Portaria do Comandante do Exército nº 691, de 14 de julho de 2014, e de acordo com o que estabelece o inciso II do art. 16 das INSTRUÇÕES GERAIS PARA O SISTEMA DE DOUTRINA MILITAR TERRESTRE – SIDOMT (EB 10-IG-01.005), 4ª Edição, aprovadas pela Portaria do Comandante do Exército nº 1498, de 21 de outubro de 2015, resolve:

Art. 1º Aprovar o Manual de Campanha EB70-MC-10.232 Guerra Cibernética, 1ª Edição, 2017, que com esta baixa.

Art. 2º Determinar que esta Portaria entre em vigor na data de sua publicação.

Gen Ex PAULO HUMBERTO CESAR DE OLIVEIRA
Comandante de Operações Terrestres

(Publicado no Boletim do Exército nº 25, de 23 de Junho de 2017)

FOLHA REGISTRO DE MODIFICAÇÃO (FRM)

NÚMERO DE ORDEM	ATO DE APROVAÇÃO	PÁGINAS AFETADAS	DATA

ÍNDICE DE ASSUNTOS

Pag

PREFÁCIO

CAPÍTULO I – INTRODUÇÃO

1.1 Finalidade.. 1-1
1.2 Considerações Iniciais.. 1-1

CAPÍTULO II – FUNDAMENTOS

2.1 Considerações Gerais.. 2-1
2.2 A Guerra Cibernética e o Conceito Operativo do Exército.............. 2-1
2.3 Conceitos Básicos.. 2-1
2.4 Princípios de Emprego... 2-3
2.5 Características da Guerra Cibernética.. 2-4
2.6 Possibilidades da Guerra Cibernética... 2-5
2.7 Limitações da Guerra Cibernética.. 2-5

CAPÍTULO III – ESTRUTURAS E RESPONSABILIDADES NA GUERRA CIBERNÉTICA

3.1 Considerações Gerais.. 3-1
3.2 Visão Sistêmica.. 3-1
3.3 Capacidades do Sistema de Guerra Cibernética do Exército.......... 3-4

CAPÍTULO IV – GUERRA CIBERNÉTICA NO CONTEXTO DAS FUNÇÕES DE COMBATE

4.1 Considerações Gerais.. 4-1
4.2 Atividades da Guerra Cibernética.. 4-1
4.3 Atividades, Tarefas e Ações da Guerra Cibernética.......................... 4-3
4.4 A Integração da Capacidade Cibernética com as Funções de Combate... 4-5

CAPÍTULO V – A GUERRA CIBERNÉTICA NAS OPERAÇÕES TERRESTRES

5.1 Considerações Gerais.. 5-1
5.2 Operações Combinadas... 5-1
5.3 Operações Ofensivas... 5-2
5.4 Operações Defensivas... 5-3
5.5 Operações de Cooperação e Coordenação com Agências................ 5-3
5.6 Operações de Informação... 5-5

REFERÊNCIAS

PREFÁCIO

A revolução tecnológica elevou o espaço cibernético a uma nova condição nos assuntos relacionados à defesa e segurança. Tal espaço é um domínio global dentro da dimensão informacional do ambiente operacional que consiste em uma rede interdependente de infraestruturas de Tecnologia da Informação e Comunicações (TIC) e de dados, incluindo a *internet*, redes de telecomunicações, sistemas de computador, processadores embarcados e controladores.

O Exército Brasileiro (EB) tem acompanhado essa revolução tecnológica e seus impactos doutrinários. Com esse foco e de forma coerente com a Doutrina Militar de Defesa Cibernética, buscou-se formular a doutrina sobre Guerra Cibernética do EB, de forma a contribuir para o desenvolvimento de capacidades nesse domínio.

No presente manual, são abordados os fundamentos da Guerra Cibernética; a integração desta às diversas funções de combate; as estruturas que compõem o Sistema de Guerra Cibernética do Exército (SGCEx) e suas respectivas responsabilidades, bem como a integração da capacidade cibernética nas operações terrestres, particularmente nas operações combinadas, nas operações básicas e nas operações de informação. O manual traz, ainda, diversos exemplos de ações cibernéticas.

Assim, esta publicação busca ampliar o conhecimento acerca dos princípios e teorias que norteiam o assunto, constituindo uma publicação no nível de concepções (nível 2), dentro do contexto da pirâmide de formulação doutrinária adotada pelo Exército.

CAPÍTULO I

INTRODUÇÃO

1.1 FINALIDADE

1.1.1 Este manual tem por finalidade estabelecer os conceitos e concepções da Doutrina de Guerra Cibernética do Exército Brasileiro (EB), proporcionando unidade de pensamento sobre o assunto, no âmbito do EB, alinhados com a Doutrina Militar de Defesa Cibernética (MD31-M-08) estabelecida pelo Ministério da Defesa (MD), e contribuindo para a atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético.

1.2 CONSIDERAÇÕES INICIAIS

1.2.1 O Brasil, como nação soberana, necessita de capacidade para se contrapor às ameaças externas, de modo compatível com sua própria dimensão e suas aspirações político-estratégicas no cenário internacional. Isso possibilita ao país a consecução de objetivos estratégicos e a preservação dos interesses nacionais, além do exercício do direito de defesa assegurado pela Constituição Federal e pelo ordenamento jurídico internacional.

1.2.2 Na atual conjuntura mundial, a sociedade brasileira, em particular a expressão militar do Poder Nacional, deverá estar permanentemente preparada, considerando os atuais e futuros contenciosos internacionais. Para tal, medidas deverão ser adotadas de modo a capacitá-la a responder oportuna e adequadamente, com proatividade, antecipando-se em face dos possíveis cenários adversos à defesa nacional.

1.2.3 Agravando ainda esse quadro, observa-se o aumento do risco de perpetração de ataques por estados, organizações e até mesmo pequenos grupos, com as mais diversas motivações.

1.2.4 Dentro desse cenário, a defesa cibernética vem se estabelecendo como atividade importante no êxito das operações militares em todos os escalões de comando. Na condição de atividade especializada, sua execução se baseia em uma concepção sistêmica, com métodos, procedimentos, características e vocabulário que lhe são peculiares.

1.2.5 Da mesma forma, a guerra cibernética, conduzida por componentes especializados das FA nos níveis operacional e tático, busca contribuir para as ações mais amplas da defesa cibernética. O Comando de Defesa Cibernética (ComDCiber), órgão central do Sistema Militar de Defesa Cibernética, coordena

e integra esses componentes das forças singulares, buscando viabilizar o exercício do Comando e Controle (C^2), por meio da proteção dos ativos de informação, além de negar o exercício do C^2 ao oponente.

1.2.6 No EB, a guerra cibernética constitui um dos multiplicadores do poder de combate, permeando as diversas funções de combate em virtude de seu caráter eminentemente transversal.

1.2.7 A partir do estabelecimento do setor cibernético, decorrente da aprovação da Estratégia Nacional de Defesa, em 2008, dois campos distintos passaram a ser reconhecidos: a segurança cibernética, a cargo da Presidência da República (PR), e a defesa cibernética, a cargo do MD, por meio das FA.

1.2.8 No contexto do Ministério da Defesa, as ações no espaço cibernético deverão ter as seguintes denominações, de acordo com o nível de decisão (conforme apresentado na Fig 1-1):
a) nível político - Segurança da Informação e Comunicações (SIC) e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo a administração pública federal (APF) direta e indireta, bem como as infraestruturas críticas da informação inerentes às infraestruturas críticas nacionais;
b) nível estratégico - Defesa Cibernética - a cargo do MD, Estado-Maior Conjunto das Forças Armadas (EMCFA) e comandos das FA, interagindo com a Presidência da República e a APF; e
c) níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das FA.

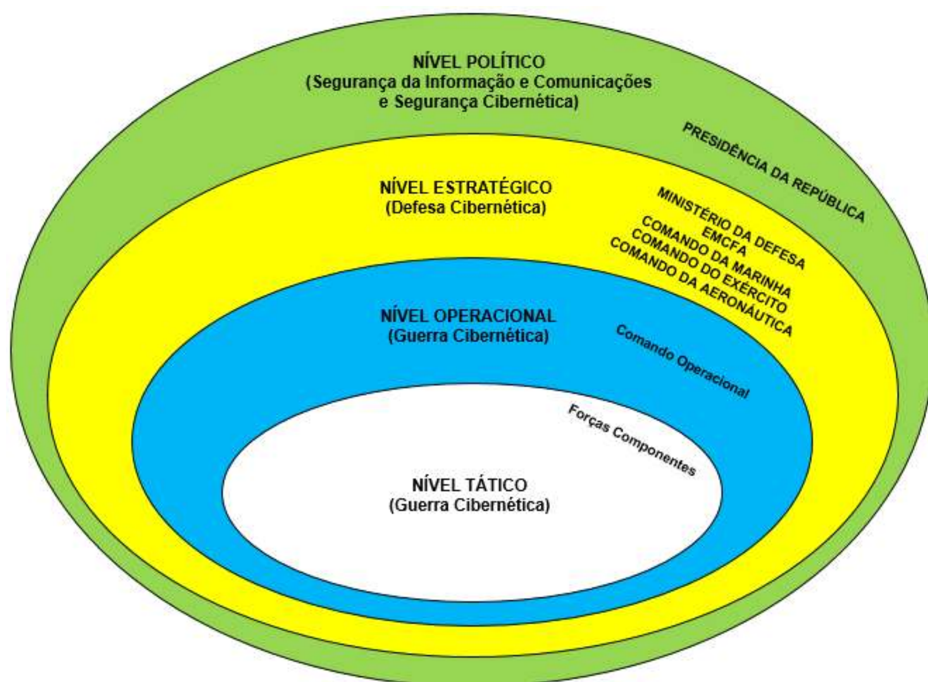


Fig 1-1 – Níveis de decisão

1.2.9 No presente manual, será apenas abordado o nível tático, no qual se insere o Exército, sendo o assunto designado como Guerra Cibernética.

CAPÍTULO II

FUNDAMENTOS

2.1 CONSIDERAÇÕES GERAIS

2.1.1 Este capítulo tem por finalidade apresentar os fundamentos da guerra cibernética no contexto do conceito operativo do Exército. A abordagem desses fundamentos abrangerá os conceitos básicos, os princípios de emprego, as características, as possibilidades e as limitações da guerra cibernética, bem como as formas de atuação no espaço cibernético.

2.2 A GUERRA CIBERNÉTICA E O CONCEITO OPERATIVO DO EXÉRCITO

2.2.1 O conceito operativo do Exército baseia-se nas operações no amplo espectro, interpretando a atuação dos elementos da Força Terrestre para obter e manter resultados decisivos nas operações, simultânea ou sucessivamente, prevenindo ameaças, gerenciando crises e solucionando conflitos armados, em situações de guerra e de não guerra. Tal conceito requer que comandantes em todos os níveis possuam alto grau de iniciativa e liderança, potencializando a sinergia das forças sob sua responsabilidade.

2.2.2 Atualmente, esse conceito operativo requer que os comandantes saibam atuar no espaço cibernético, empregando a capacidade militar terrestre cibernética. Tais capacidades estão presentes em todas as operações e permeiam todas as seis funções de combate. Assim, os fundamentos apresentados a seguir propiciam aos comandantes uma melhor compreensão do assunto, com o propósito de facilitar o emprego dessas capacidades em apoio ao combate.

2.3 CONCEITOS BÁSICOS

2.3.1 AMEAÇA CIBERNÉTICA – causa potencial de um incidente indesejado, que pode resultar em dano ao espaço cibernético de interesse.

2.3.2 ARTEFATO CIBERNÉTICO – equipamento ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração e ataque cibernéticos.

2.3.3 ATIVOS DE INFORMAÇÃO – meios de armazenamento, transmissão e processamento de dados e informação, os equipamentos necessários a isso (computadores, equipamentos de comunicações e de interconexão), os

sistemas utilizados para tal, os sistemas de informação de um modo geral, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

2.3.4 CIBERNÉTICA – termo que se refere a comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação.

2.3.5 DEFESA CIBERNÉTICA – conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo MD, com as finalidades de proteger os sistemas de informação (Sist Info) de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e comprometer os sistemas de informação do oponente.

2.3.6 ESPAÇO CIBERNÉTICO – espaço virtual composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas e/ou armazenadas.

2.3.7 FONTE CIBERNÉTICA – recurso que possibilita a obtenção de dados no espaço cibernético, utilizando-se ações de busca ou coleta, normalmente realizadas com auxílio de ferramentas computacionais. A fonte cibernética poderá ser integrada a outras fontes (humanas, imagens e sinais) para produção de conhecimento de inteligência.

2.3.8 GUERRA CIBERNÉTICA – corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C2 AO adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de TIC para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sist Info. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação às TIC.

2.3.9 INFRAESTRUTURA CRÍTICA DA INFORMAÇÃO – subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do estado e a segurança da sociedade.

2.3.10 PODER CIBERNÉTICO – capacidade de utilizar o espaço cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder.

2.3.11 RESILIÊNCIA CIBERNÉTICA – capacidade de manter as infraestruturas críticas da informação operando sob condições de ataque cibernético ou de restabelecê-las após uma ação adversa.

2.3.12 RISCO CIBERNÉTICO – probabilidade de ocorrência de um incidente cibernético associado à magnitude do dano por ele provocado.

2.3.13 SEGURANÇA CIBERNÉTICA – arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas.

2.3.14 SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (SIC) – ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações.

2.3.14.1 Disponibilidade – propriedade segundo a qual a informação deve ser acessível e utilizável sob demanda por uma pessoa física ou por determinado sistema, órgão ou entidade.

2.3.14.2 Integridade – propriedade segundo a qual a informação não deve ser modificada ou destruída de maneira não autorizada ou acidental.

2.3.14.3 Confidencialidade – propriedade segundo a qual a informação não deve estar disponível ou ser revelada a pessoa física, sistema, órgão ou entidade não autorizados ou não credenciados.

2.3.14.4 Autenticidade – propriedade segundo a qual a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física ou por um determinado sistema, órgão ou entidade.

2.3.15 SETOR CIBERNÉTICO – um dos três setores de importância estratégica para a defesa nacional, de acordo com a Estratégia Nacional de Defesa, abrangendo as pessoas, instalações, infraestruturas e recursos tecnológicos, de nível estratégico, necessários para que as FA possam atuar em rede com segurança, tais como o Sistema Militar de Comando e Controle (SISMC[2]), sistemas de armas/vigilância e sistemas administrativos que possam afetar as atividades operacionais.

2.4 PRINCÍPIOS DE EMPREGO

2.4.1 Os tradicionais princípios de guerra aplicam-se a todos os tipos de operações militares, incluindo as ações cibernéticas. As peculiaridades da guerra cibernética, no entanto, impõem que outros princípios sejam considerados.

2.4.2 São princípios de emprego da guerra cibernética:
a) princípio do efeito;
b) princípio da dissimulação;
c) princípio da rastreabilidade; e
d) princípio da adaptabilidade.

2.4.2.1 Princípio do Efeito - as ações cibernéticas devem produzir efeitos

que se traduzam em vantagem estratégica, operacional ou tática que afetem o mundo real, mesmo que esses efeitos não sejam cinéticos.

2.4.2.2 Princípio da Dissimulação – medidas ativas devem ser adotadas para se dissimular no espaço cibernético, dificultando a rastreabilidade das ações cibernéticas ofensivas e exploratórias levadas a efeito contra os sistemas de informação oponentes. Objetiva-se, assim, mascarar a autoria e o ponto de origem dessas ações.

2.4.2.3 Princípio da Rastreabilidade – medidas efetivas devem ser adotadas para se detectar ações cibernéticas ofensivas e exploratórias contra os sistemas de TIC amigos. Quase sempre, as ações cibernéticas envolvem a movimentação ou a manipulação de dados, as quais podem ser registradas nos sistemas de TIC.

2.4.2.4 Princípio da Adaptabilidade – consiste na capacidade da guerra cibernética de adaptar-se à característica de mutabilidade do espaço cibernético, mantendo a proatividade mesmo diante de mudanças súbitas e imprevisíveis.

2.5 CARACTERÍSTICAS DA GUERRA CIBERNÉTICA

2.5.1 A guerra cibernética possui as mesmas características da defesa cibernética, sendo adaptadas para os níveis operacional e tático.

2.5.2 INSEGURANÇA LATENTE - nenhum sistema computacional é totalmente seguro, tendo em vista que as vulnerabilidades nos ativos de informação serão sempre objeto de exploração por ameaças cibernéticas.

2.5.3 ALCANCE GLOBAL - a guerra cibernética possibilita a condução de ações em escala global, simultaneamente, em diferentes frentes. Limitações físicas de distância e espaço não se aplicam ao espaço cibernético.

2.5.4 VULNERABILIDADE DAS FRONTEIRAS GEOGRÁFICAS - as ações de guerra cibernética não se limitam a fronteiras geograficamente definidas, pois os agentes podem atuar a partir de qualquer local e provocar efeito em qualquer lugar.

2.5.5 MUTABILIDADE - não existem leis de comportamento imutáveis no espaço cibernético, pois podem adaptar-se às condições ambientais e da criatividade do ser humano.

2.5.6 INCERTEZA - as ações cibernéticas podem ou não gerar os efeitos desejados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados.

2.5.7 DUALIDADE - na guerra cibernética, as mesmas ferramentas podem ser usadas por atacantes e administradores de sistemas com finalidades distintas: uma ferramenta que busque as vulnerabilidades do sistema, por exemplo, pode

ser usada por atacantes para encontrar pontos que representem oportunidades de ataque em seus sistemas-alvo e, por administradores, para descobrir as vulnerabilidades de equipamentos e de redes.

2.5.8 FUNÇÃO DE APOIO – as ações cibernéticas não são um fim em si mesmas, sendo empregadas para apoiar a condução das operações militares.

2.5.9 ASSIMETRIA – baseada no desbalanceamento de forças, causado pela introdução de um ou mais elementos de ruptura tecnológicos, metodológicos ou procedimentais que podem causar danos tão prejudiciais quanto aqueles perpetrados por estados ou organizações com maiores condições econômicas, por exemplo.

2.6 POSSIBILIDADES DA GUERRA CIBERNÉTICA

2.6.1 São possibilidades da guerra cibernética:
a) atuar no espaço cibernético, por meio de ações ofensivas, defensivas e exploratórias;
b) cooperar na produção do conhecimento de inteligência por meio dos dados obtidos da fonte cibernética;
c) atingir sistemas de informação de um oponente sem limitação de alcance físico e exposição de tropa;
d) cooperar com a segurança cibernética, inclusive de órgãos externos ao MD, mediante solicitação ou no contexto de uma operação;
e) cooperar com o esforço de mobilização para assegurar a capacidade dissuasória da guerra cibernética;
f) facilitar a obtenção da surpresa, com base na exploração das vulnerabilidades dos sistemas de informação do oponente;
g) realizar ações contra oponentes com poder de combate superior; e
h) realizar ações com custos significativamente menores do que aqueles envolvidos nas operações militares nos demais domínios.

2.7 LIMITAÇÕES DA GUERRA CIBERNÉTICA

2.7.1 São limitações da guerra cibernética:
a) restrita capacidade de identificação da origem e atribuição de responsabilidades por ataques cibernéticos;
b) restrita eficácia das ações cibernéticas defensivas, devido à existência de vulnerabilidades nos sistemas computacionais;
c) restrita capacidade de gestão de pessoas, particularmente no que concerne à identificação, seleção, capacitação e retenção de talentos;
d) dificuldade de acompanhamento da evolução tecnológica na área cibernética; e
e) possibilidade de ser surpreendido com base nas vulnerabilidades dos próprios sistemas de informação.

CAPÍTULO III

ESTRUTURAS E RESPONSABILIDADES NA GUERRA CIBERNÉTICA

3.1 CONSIDERAÇÕES GERAIS

3.1.1 O Sistema de Guerra Cibernética do Exército (SGCEx) é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de guerra cibernética, assegurando o seu uso efetivo pelo Exército Brasileiro, bem como impedindo ou dificultando a utilização do espaço cibernético pelo oponente.

3.1.2 O SGCEx visa à proteção cibernética do Sistema de Comando e Controle do Exército, assegurando a capacidade de atuar em rede com segurança, bem como a coordenar e a integrar a proteção das infraestruturas críticas da informação sob responsabilidade do Exército.

3.2 VISÃO SISTÊMICA

3.2.1 A fim de que se tenha a melhor compreensão da inserção do SGCEx em um contexto mais amplo, a Fig 3-1 apresenta a concepção do Sistema Militar de Defesa Cibernética (SMDC), do qual o SGCEx faz parte.

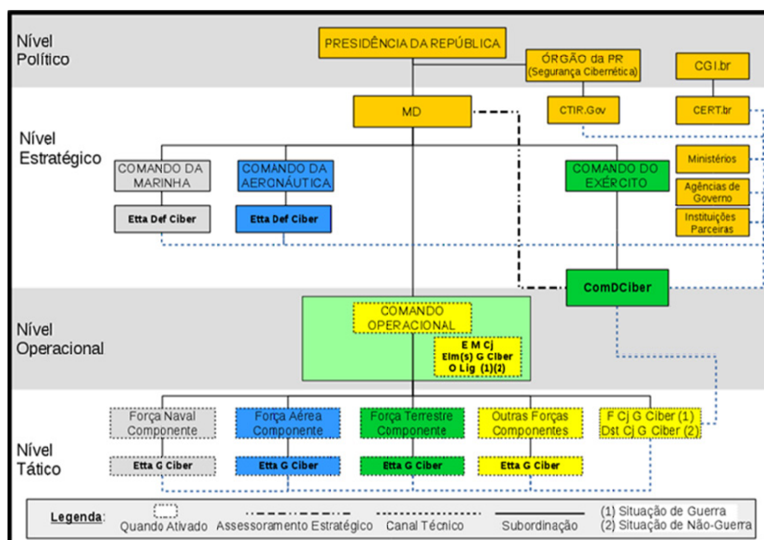


Fig 3-1 – Sistema Militar de Defesa Cibernética (SMDC)

3.2.2 No nível tático, quando for ativada a Estrutura Militar de Defesa (Etta Mi D), a Força Terrestre Componente (FTC) será apoiada por uma Etta G Ciber. Essa estrutura engloba os elementos do 1º Batalhão de Guerra Eletrônica (BGE), o Batalhão de Comunicações (B Com), o Batalhão de Comunicações e Guerra Eletrônica (B Com GE), o Batalhão de Inteligência Militar (BIM), a Companhia de Comando e Controle (Cia C^2) e as Companhias de Comunicações (Cia Com), de acordo com o que é apresentado na Tab 3-1.

3.2.3 Os elementos das OM acima elencadas integram a estrutura do estado-maior da FTC. Em um momento determinado, de acordo com a missão da FTC, o comando poderá variar a Estrutura de Guerra Cibernética.

3.2.4 Em uma situação de conflito, dependendo da missão e de acordo com os fatores da decisão, a capacidade militar terrestre cibernética da FTC será operacionalizada pelo emprego das estruturas operativas apresentadas na Tab 3-1, cada qual com suas respectivas ações cibernéticas.

3.2.5 O planejamento e o assessoramento relacionado às ações cibernéticas em prol da FTC podem ser realizados pelo comandante do BGE, de um B Com, de um B Com GE, da Cia C^2 ou das Cia Com, dependendo da composição da FTC. O comandante do BIM é responsável pelo planejamento e assessoramento relacionados às ações de exploração cibernética. Essas ações são de interesse para as operações de inteligência conduzidas em proveito da manobra da FTC e para a produção do conhecimento de inteligência.

Estrutura	Atq	Expl	Prot	Responsabilidades
Batalhão de Guerra Eletrônica (BGE)	X	X	X	Realiza a exploração e o ataque cibernéticos em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética e de ataque cibernético em prol da FTC.
Batalhão de Comunicações (B Com)			X	Realiza a proteção cibernética dos sistemas de informação do grande comando apoiado. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética da FTC.
Batalhão de Comunicações e Guerra Eletrônica (B Com GE)		X	X	Realiza a proteção cibernética dos sistemas de informação da FTC apoiada, bem como a exploração cibernética (com limitações) em proveito deste escalão. O comandante do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética e de exploração cibernética da FTC, quando o BGE não estiver presente.
Batalhão de Inteligência Militar (BIM)		X	X	Realiza a exploração cibernética em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. Seu comandante será responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética de interesse para as operações de inteligência conduzidas em proveito da manobra da FTC e para a produção do conhecimento de inteligência.
Companhia de Comando e Controle (Cia C2)			X	Realiza a proteção cibernética dos postos de comando da Força Terrestre Componente.
Companhia de Comunicações (Cia Com)			X	Realiza a proteção cibernética dos sistemas de informação de uma grande unidade.
OM integrantes da FTC			X	Realizam a proteção cibernética (somente preventiva) dos sistemas de informação da OM.

Tab 3-1 – Estruturas operativas de G Ciber, suas atividades cibernéticas e responsabilidades

3.2.6 Em operações, as atividades de G Ciber poderão ser complementadas pelas seguintes OM:

a) Comando de Defesa Cibernética (ComDCiber);

b) Centro de Defesa Cibernética (CDCiber);

c) Centro Integrado de Telemática do Exército (CITEx);

d) Centros de Telemática de Área (CTA) e Centros de Telemática (CT);
e) Centro de Desenvolvimento de Sistemas (CDS);
f) Centro de Inteligência do Exército (CIE); e
g) outras OM, conforme a situação.

3.3 CAPACIDADES DO SISTEMA DE GUERRA CIBERNÉTICA DO EXÉRCITO

3.3.1 Capacidade é a aptidão requerida a uma força ou organização militar, para que possa cumprir determinada missão ou tarefa. É obtida a partir do desenvolvimento de um conjunto de sete fatores determinantes, inter-relacionados e indissociáveis: doutrina, organização (e processos), adestramento, material (e sistemas), educação, pessoal e infraestrutura. As capacidades operativas do SGCEx são descritas na Tab a seguir.

3.3.2 CAPACIDADES OPERATIVAS

3.3.2.1 As capacidades operativas (CO) da capacidade militar terrestre cibernética são três: a proteção cibernética, o ataque cibernético e a exploração cibernética (Tab 3-2).

Capacidade Operativa	Descrição
Proteção Cibernética	Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.
Ataque Cibernético	Ser capaz de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente.
Exploração Cibernética	Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

Tab 3-2 – Capacidades do SGCEx

3.3.2.2 As atividades, tarefas e ações correspondentes às capacidades operativas serão abordadas no capítulo IV.

CAPÍTULO IV

A GUERRA CIBERNÉTICA NO CONTEXTO DAS FUNÇÕES DE COMBATE

4.1 CONSIDERAÇÕES GERAIS

4.1.1 O presente capítulo tem o propósito de apresentar as atividades de guerra cibernética, incluindo as correspondentes tarefas e ações. Abordará, também, a integração da capacidade cibernética às funções de combate.

4.1.2 Uma função de combate é um conjunto relativamente homogêneo de atividades e tarefas afins, que atendem a uma finalidade comum, além dos sistemas empregados na sua execução (pessoas, organizações, informações e processos), que orienta o preparo e o emprego dos meios no cumprimento de suas missões.

4.1.3 As funções de combate são seis: movimento e manobra; inteligência; fogos; proteção; comando e controle; e logística.

4.2 ATIVIDADES DA GUERRA CIBERNÉTICA

4.2.1 Durante a fase de planejamento das operações, os comandantes e seus estados-maiores identificam todas as atividades a cumprir no espaço cibernético. Em seguida selecionam as tarefas mais adequadas a serem conduzidas e iniciam o detalhamento de como conduzir as ações cibernéticas necessárias ao cumprimento da missão.

4.2.2 Pelas especificidades da G Ciber, as atividades têm a mesma nomenclatura das capacidades operativas. As atividades da guerra cibernética são as seguintes:

4.2.3 ATAQUE CIBERNÉTICO

4.2.3.1 É a atividade que tem o objetivo de interromper, negar o uso, degradar, corromper ou destruir sistemas computacionais ou informações armazenadas em dispositivos e redes computacionais e de comunicações de interesse.

4.2.3.2 O ataque cibernético emprega códigos computacionais, podendo ser conduzido no espectro eletromagnético ou em dispositivos de rede, tais como: servidores, *bridges*, *firewalls*, sensores, protocolos, sistemas operacionais e *hardwares* associados a computadores. Pode, ainda, ser direcionado contra sistemas de armas do oponente.

4.2.3.3 O ataque cibernético deve ser consistente com o arcabouço legal e normativo vigente, requerendo coordenação e sincronização com as ações das funções de combate.

4.2.3.4 Pode ser empregado em conjunto com medidas de ataque eletrônico (MAE) e fogos contra alvos priorizados. Para isso, cresce de importância a integração com a inteligência, no sentido de coletar e buscar informações sobre esses alvos, no que concerne ao espaço cibernético.

4.2.3.5 O ataque cibernético pode abranger ações da atividade de exploração cibernética. No contexto de um ataque cibernético, as ações da atividade de exploração cibernética visam a preparar o ataque, constituindo-se em passos iniciais e intermediários para a consecução deste.

4.2.3.6 Quanto à origem dos ataques, estes podem ser externos, internos (ou ataques de *insiders*) e transitivos.

4.2.3.6.1 Nos externos, o atacante não pertence à instituição.

4.2.3.6.2 Os ataques internos são realizados por pessoal interno ou por elementos fisicamente infiltrados que tiveram acesso a informações em nível superior ao necessário. Eles podem causar interrupção em sistemas críticos, perda de informação classificada e, consequentemente, danos à reputação da organização.

4.2.3.6.3 Os ataques transitivos são realizados contra alvos que possuem uma cadeia de confiança entre si, o que lhes dificulta a capacidade de limitar o acesso proveniente da organização parceira, facilitando, assim, a ação do atacante.

4.2.3.7 A determinação da origem dos ataques denomina-se atribuição. Cabe ressaltar que, muitas vezes, a atribuição de um ataque é complexa, uma vez que, normalmente, a origem costuma ser mascarada pelo atacante.

4.2.4 EXPLORAÇÃO CIBERNÉTICA

4.2.4.1 Visa à obtenção (incluindo busca e coleta) de informações, nos sistemas de informação de interesse, a fim de obter a consciência situacional do ambiente cibernético. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

4.2.4.2 As informações a serem obtidas podem incluir dados técnicos de sistemas, *modus operandi*, ferramentas, formas de ataque e informações sobre a liderança. dos principais grupos e organizações oponentes.

4.2.4.3 Essa atividade permite, também, de forma proativa, identificar antecipadamente possíveis ações hostis em planejamento. Os dados gerados devem ser tempestivamente analisados e repassados aos detentores dos ativos

em risco, por alertas ou notificações de eventos de segurança.

4.2.4.4 Assim como o ataque cibernético, a exploração cibernética deve seguir a orientação do arcabouço normativo e legal em vigor.

4.2.5 PROTEÇÃO CIBERNÉTICA

4.2.5.1 Visa neutralizar o ataque e a exploração cibernética oponentes contra os dispositivos computacionais, as redes de computadores e de comunicações amigos. É uma atividade de caráter permanente.

4.2.5.2 Tais ações de proteção cibernética incluem a detecção, a identificação e a resposta a ações que foram realizadas ou que estão prestes a serem conduzidas pelo oponente.

4.2.5.3 No contexto da proteção cibernética, podem ser empregadas determinadas ações de ataque cibernético e de exploração cibernética. Por exemplo, podem ser mencionadas as ações realizadas nos testes de vulnerabilidades, incluindo testes de invasão, a fim de testar e avaliar a proteção cibernética dos sistemas de informação quanto ao grau de resiliência.

4.2.5.4 No âmbito do Exército Brasileiro, a proteção cibernética tem o propósito de proteger as redes do Sistema de Comando e Controle do Exército (SC^2Ex).

4.2.5.5 Na cibernética, o conceito de defesa em profundidade consiste em introduzir múltiplas camadas de proteção que permitam reduzir a probabilidade de comprometimento dos sistemas de informação amigos. No caso de que uma das camadas falhe, mitiga-se, assim, o impacto do ataque ou da exploração cibernética oponente sobre esses sistemas.

4.3 ATIVIDADES, TAREFAS E AÇÕES DA GUERRA CIBERNÉTICA

4.3.1 A Tab 4-1 mostra as atividades e tarefas da guerra cibernética.

Atividade	Tarefa
Proteção Cibernética	**Gestão de Riscos** Gerenciar as relações entre ativos de informação, patrimônio digital, ameaças, vulnerabilidades, impactos, probabilidade de ocorrência de incidentes de segurança da informação e riscos. Estabelece o nível de alerta cibernético correspondente e executa o tratamento, a comunicação e a monitoração contínua desses riscos.
	Consciência Situacional Monitorar sistematicamente o espaço cibernético de interesse do EB no tocante à possibilidade de concretização de ameaça, de modo a estar em condições de decidir e aplicar as ações requeridas conforme as condições do espaço cibernético.
	Defesa Ativa Detectar, identificar, avaliar e neutralizar vulnerabilidades nas redes de computadores e sistemas de informação em uso pelo EB, antes que elas sejam exploradas. Mediante ordem, desencadear ações ofensivas contra a fonte da ameaça, mesmo que localizada fora do espaço cibernético defendido.
	Pronta Resposta Reagir prontamente às ameaças identificadas, observando os diferentes níveis de alerta cibernético (grau de risco).
	Forense Digital Coletar e examinar evidências digitais em redes e sistemas de informação de interesse do EB.
	Teste de Artefatos Cibernéticos Testar, simular, analisar, avaliar e homologar artefatos e sistemas cibernéticos.
	Conformidade de SIC Verificar a observância de aspectos legais, normativos e procedimentais de SIC no âmbito do SGCEx.
	Gestão de Incidentes de Redes Coordenar o tratamento de incidentes nas redes de interesse, acompanhar a solução e acionar procedimentos.
	Controle de Acesso Permitir que os administradores e gerentes determinem o que os indivíduos podem acessar, de acordo com sua credenciais de segurança, após a autorização, a autenticação, o controle e a monitoração dessas atividades.
	Proteção das comunicações Examinar os sistemas de comunicações internos, externos, públicos e privados; estruturas de rede; dispositivos; protocolos; acesso remoto e administração.
	Emprego de Criptografia Empregar técnicas, abordagens e tecnologias de criptografia.
	Implementação de controles de segurança Controlar atividades de pessoal e procedimentos de segurança, na utilização dos sistemas necessários às atividades na área cibernética.
	Segurança Física Autorizar a entrada e estabelecer os procedimentos de segurança do ambiente operativo, a fim de proteger instalações, equipamentos, dados, mídias e pessoal contra ameaças físicas aos ativos de informação.
	Gestão da Continuidade da Missão e Recuperação de Desastres Preservar as atividades operativas por ocasião da ocorrência de interrupções ou de catástrofes.

Atividade	Tarefa
Ataque Cibernético	**Reconhecimento** Investigar em fontes abertas para obter informações sobre o alvo.
	Escaneamento (*Scanning*) Encontrar falhas na proteção cibernética do alvo.
	Exploração da Vulnerabilidade Realizar ações como: obter acesso, degradar uma aplicação ou negar acesso para outros usuários.
	Manutenção do acesso Manipular *software* instalado no sistema alvo com objetivo de disponibilizar um *backdoor* para acesso futuro.
	Cobertura de rastros Ocultar as ações realizadas no sistema alvo com objetivo de impedir ou dificultar que usuários e/ou administradores identifiquem as ações de um atacante.
Exploração Cibernética	**Inteligência Cibernética** Realizar ações de busca e de coleta de dados no espaço cibernético, para a produção do conhecimento de Inteligência.

Tab 4-1 – Atividades e Tarefas da Guerra Cibernética

4.3.2 As tarefas da atividade de ataque cibernético, por serem sequenciais, são também conhecidas como fases do ataque cibernético.

4.3.3 As ações a serem executadas em cada tarefa de guerra cibernética serão detalhadas nos manuais técnicos das atividades de G Ciber.

4.4 A INTEGRAÇÃO DA CAPACIDADE CIBERNÉTICA COM AS FUNÇÕES DE COMBATE

4.4.1 A guerra cibernética provê apoio ao combate, potencializando os efeitos das atividades das funções de combate. A seguir, serão apresentados os principais aspectos a serem considerados na integração com cada função de combate.

4.4.2 MOVIMENTO E MANOBRA

4.4.2.1 As ações de guerra cibernética podem anteceder ações cinéticas no Teatro de Operações (TO). Podem causar a negação de serviços mantidos pelo oponente ou a desinformação à tropa inimiga – no contexto das operações de Informação - facilitando as ações das tropas. As ações de guerra cibernética podem amplificar as ações cinéticas no TO.

4.4.2.2 Por meio de ações exploratórias, é possível realizar um exame das táticas, técnicas e procedimentos (TTP) do oponente no espaço cibernético. Observando esses padrões, pode-se realizar uma análise do curso da manobra e do movimento do oponente.

4.4.2.3 Por intermédio de ações de proteção cibernética, busca-se garantir a segurança das redes de comando e controle e infraestruturas de TIC para apoiar o movimento e a manobra, propiciando a sincronização das ações cinéticas, proporcionando ao comandante a segurança, a liberdade de ação na operação e importantes vantagens no espaço de batalha.

4.4.3 INTELIGÊNCIA

4.4.3.1 Devem-se levantar as necessidades de conhecimento a respeito do oponente sobre doutrina, estruturas dedicadas à atividade de guerra cibernética e possíveis alvos (sistemas e infraestruturas) para as ações de exploração e ataque cibernético.

4.4.3.2 A integração da G Ciber com a inteligência é realizada da seguinte forma:
a) coleta e busca de dados de potenciais ameaças ou adversários;
b) análise de dados coletados sobre redes e ativos de informação; e
c) compartilhamento de dados em múltiplos níveis de segurança.

4.4.4 FOGOS

4.4.4.1 Os ataques de fogos cinéticos e não cinéticos – os ataques cibernéticos estão classificados nesta última categoria - podem ser executados simultaneamente para causar efeitos complementares sobre um mesmo alvo.

4.4.4.2 Deve ser formulada uma lista de possíveis alvos existentes no interior da área da FTC, para exploração e ataque cibernéticos, com base no levantamento anterior realizado por ocasião da análise de G Ciber. Uma vez definida a lista de alvos, os ataques cibernéticos podem oferecer ao planejamento de fogos uma melhor opção para causar os efeitos pretendidos em alvos inimigos, com menores efeitos colaterais no ambiente físico.

4.4.4.3 As ações de exploração cibernética podem fornecer informações sobre alvos pretendidos, sejam eles cibernéticos ou não, contribuindo para a decisão de alvos compensadores para os fogos de artilharia.

4.4.5 COMANDO E CONTROLE (C^2)

4.4.5.1 A consciência situacional na área cibernética colabora e deve ser integrada à consciência situacional proporcionada pelo Sistema de Comando e Controle da FTC, propiciando a construção de um cenário operativo comum.

4.4.5.2 São exemplos de informações relevantes para a consciência situacional cibernética:
a) informações em tempo real sobre capacidades do adversário, elementos infiltrados;
b) planos, intenções e ações em redes de unidades do oponente;
c) serviços, sistemas e os impactos potenciais sobre a missão e sobre as forças amigas;
d) considerações legais;

e) ganhos ou perdas de inteligência;
f) riscos associados com as decisões tomadas e ações realizadas no ciberespaço e no espectro eletromagnético; e
g) outras informações obtidas no espaço cibernético de interesse para as operações.

4.4.6 PROTEÇÃO

4.4.6.1 A atividade de G Ciber pode fornecer subsídios, dados e informações sobre a localização de pontos sensíveis a serem protegidos pelas tropas.

4.4.6.2 A G Ciber se integra à função de combate proteção por meio das ações de proteção cibernética dos sistemas de informação da FTC. É fundamental manter a disponibilidade, integridade, confiabilidade e autenticidade das informações que trafegam ou que são armazenadas nos sistemas de informação.

4.4.6.3 Deve-se formular uma lista preliminar de ativos de informação, no interior da área de operações da FTC, que necessitam ser protegidos por ações de proteção cibernética.

4.4.6.4 A G Ciber contribui, também, para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior da área de operações da FTC, com o propósito de buscar a garantia de sua segurança e de seu funcionamento.

4.4.7 LOGÍSTICA

4.4.7.1 O planejamento de G Ciber deve fornecer dados relacionados a possíveis ataques inimigos que possam impactar o suprimento e ressuprimento da tropa.

4.4.7.2 Além disso, o fornecimento de equipamentos e a mobilização de pessoal são alguns exemplos da integração da capacidade cibernética à logística.

4.4.7.3 As capacidades e ativos da informação não providos pela logística própria do Exército poderão ser complementados por meio da mobilização.

4.4.7.4 No contexto da mobilização, em situações de normalidade ou de crise, se a situação assim exigir, poderá haver o recrutamento de especialistas em segurança cibernética em instituições públicas e privadas, acadêmicas ou não, a fim de atuarem colaborativamente junto às estruturas de G Ciber da FTC, sob coordenação e integração dos especialistas dessas estruturas.

CAPÍTULO V

A GUERRA CIBERNÉTICA NAS OPERAÇÕES TERRESTRES

5.1 CONSIDERAÇÕES GERAIS

5.1.1 Este capítulo aborda as formas de emprego de ações cibernéticas, nas operações conjuntas e interações com os diversos órgãos e forças que atuem nesse setor.

5.1.2 O espaço cibernético constitui um dos cinco domínios operacionais e permeia todos os demais: o terrestre, o marítimo, o aéreo e o espacial. Esse domínio pode alavancar as capacidades de todos os outros, e a combinação dos meios e a convergência de esforços tornam-se indispensáveis para que seja obtido o máximo rendimento das forças disponíveis.

5.1.3 No espaço cibernético, devido à complexidade e a permeabilidade dos sistemas de informação, torna-se imprescindível a realização de esforços para que haja uma organização e definição de responsabilidades. É necessária, ainda, a integração dos diversos setores envolvidos na operação, desenvolvimento e proteção dos sistemas computacionais.

5.1.4 Em situação de normalidade, caberá a cada órgão, civil ou militar, governamental ou privado, que possua atribuições ou seja integrante do espaço cibernético, realizar todas as ações necessárias para assegurar a existência e a continuidade da sociedade da informação da nação, garantindo e protegendo seus ativos de informação e suas infraestruturas críticas.

5.1.5 As ações cibernéticas são aplicáveis no amplo espectro dos conflitos. Normalmente a G Ciber participa das combinações simultâneas de atitudes realizadas pela FTC. Nesse contexto, é importante garantir o perfeito funcionamento dos sistemas e das estruturas críticas de informação e comunicações e a salvaguarda de bancos de dados estratégicos.

5.2 OPERAÇÕES COMBINADAS

5.2.1 Elementos especializados em G Ciber podem compor tropas da F Ter que integram arranjos internacionais de defesa coletiva, de acordo com os interesses nacionais. Esses arranjos consistem na formação de coalizões de forças multinacionais para o restabelecimento da ordem jurídica internacional.

5.2.2 O uso do espaço cibernético de uma nação requer coordenação e

negociação formais, buscando desenvolver a capacidade de interoperabilidade. As ações cibernéticas desenvolvidas em missões multinacionais requerem um grande esforço de integração. Esses esforços irão mitigar possíveis complicações causadas por diferenças de políticas ou quanto aos dispositivos e sistemas de integração e de compartilhamento de informações.

5.2.3 Diferenças entre padrões e entre legislações referentes à soberania do ciberespaço podem afetar a disposição e a legalidade de participação de um país em uma operação. Portanto, alguns países podem recusar-se a participar, enquanto outros podem realizar suas próprias ações separadamente.

5.2.4 A conectividade e a integração são essenciais quando forças multinacionais trabalham em apoio mútuo nas operações. Algumas incompatibilidades ou disparidades de equipamentos e programas, além de políticas de garantia e segurança da informação, podem causar brechas de segurança ou de capacidade operativa.

5.2.5 Com o objetivo de minimizar uma provável lentidão para alcançar os objetivos, deve-se realizar o planejamento antecipado sobre os requisitos técnicos de integração, visando a evitar as disparidades ou incompatibilidades.

5.2.6 No espaço cibernético, o compartilhamento de informações com aliados e parceiros multinacionais é muito importante durante a consecução de operações combinadas. Ao conduzir ações cibernéticas, todas as tropas participantes devem adotar os procedimentos e as políticas estabelecidos para a garantia do funcionamento e da proteção de sistemas de informação e de redes de computadores.

5.2.7 Cada país tem soberania sobre o espaço cibernético em sua delimitação geográfica. Portanto, o uso do ciberespaço de uma nação requer coordenação e negociação formais. Essa coordenação busca desenvolver a capacidade de interoperabilidade no ciberespaço.

5.3 OPERAÇÕES OFENSIVAS

5.3.1 A complexidade das redes e sua rápida adaptação ao desenvolvimento das ações exigem um minucioso planejamento. Para as ações cibernéticas, serão empregados todos os recursos, com o objetivo de criar soluções alternativas para o cumprimento da missão.

5.3.2 Nas operações ofensivas, crescem de importância as ações de ataque e de exploração cibernética.

5.3.3 Em coordenação com os fogos e com a guerra eletrônica, deve-se elaborar uma lista de alvos cibernéticos (LIA Ciber) e uma lista priorizada de alvos cibernéticos (LIPA Ciber).

5.3.4 As diferentes tarefas de ataque descritas no capítulo 4 podem ser realizadas, no nível tático, em apoio às operações da FTC, observando-se a integração com as várias funções de combate.

5.3.5 A estrutura de guerra Cibernética da FTC pode, também, realizar tarefas ofensivas para negar serviço ou prejudicar o funcionamento das infraestruturas críticas do oponente localizadas no interior de sua zona de ação.

5.3.6 Tal estrutura pode, ainda, realizar ações de exploração cibernética, para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo. Isso facilitará o planejamento das ações de ataque cibernético e a produção de dados para a inteligência de fonte cibernética.

5.3.7 As ações de proteção cibernética têm caráter permanente em todas as fases da operação. A proteção cibernética dos sistemas de informação é essencial para o seu eficaz exercício durante o ataque. Redundâncias e outros mecanismos contra falhas de segurança dos sistemas de informação devem proporcionar a continuidade da missão.

5.4 OPERAÇÕES DEFENSIVAS

5.4.1 Nas operações defensivas prevalecem as ações de proteção cibernética. A manutenção dessas ações em relação aos sistemas de informação em uma operação costuma ser crítica. A G Ciber é fundamental em uma defesa móvel em razão dos seguintes fatores:
a) intenso fluxo da informação;
b) rapidez na tomada de decisões e na difusão das ordens; e
c) coordenação de todas as funções de combate em tempo e espaço.

5.4.2 As ações de exploração cibernética e de ataque cibernético podem ser conduzidas, desde que não denunciem a posição, o endereço lógico e as intenções das tropas amigas.

5.4.3 Estabelecido o contato com o inimigo, as ações cibernéticas realizadas via rádio terão maior liberdade de uso, mas sempre com o emprego de medidas preventivas de proteção cibernética.

5.5 OPERAÇÕES DE COOPERAÇÃO E COORDENAÇÃO COM AGÊNCIAS

5.5.1 No ambiente cibernético, dada a permeabilidade dos sistemas de informação e a criticidade dos demais serviços, no campo civil ou militar, a interação com outros órgãos torna-se imprescindível para ambas as partes, mediante a atuação colaborativa, considerando-se as particularidades e as

possibilidades de cada parte.

5.5.2 No contexto das operações de estabilização, ações de ataque cibernético podem ser realizadas para desarticular o Comando e Controle das forças oponentes e colaborar com as operações de informação. Pode ser empregada a negação de serviço ou a exploração cibernética de *sites*, *blogs* e redes sociais utilizados pelo adversário.

5.5.2.1 Quando a F Ter participar de Op sob a égide de organismos internacionais, as ações cibernéticas devem seguir os dispositivos legais, sendo válido o disposto no item 5.2 Operações Combinadas. Essas ações cibernéticas devem ser empregadas de forma a potencializar os efeitos das ações das operações de estabilização, integrando-as com as Op Info.

5.5.3 No contexto das Op de Ap a Agências, a G Ciber busca a integração com órgãos de interesse, desde a situação de normalidade institucional, com a finalidade de facilitar as ações decorrentes de uma evolução para situações de crise ou conflito, levando-se em consideração o amplo espectro dos conflitos.

5.5.3.1 O Com D Ciber, como órgão central do SMDC, mantém o canal técnico para coordenação e integração com os órgãos de interesse envolvidos nas atividades de guerra cibernética.

5.5.3.2 A necessidade de coordenação entre as agências define a estrutura a ser organizada para o cumprimento da missão, seja no nível estratégico - a cargo do Destacamento Conjunto de Defesa Cibernética (Dst Cj Def Ciber) -, seja nos níveis operacional - de responsabilidade da Força Conjunta de Guerra Cibernética (F Cj G Ciber) - e tático (a cargo da Estrutura de G Ciber de cada força componente). Para tanto, na composição dessa estrutura estão presentes elementos de ligação interagências e elementos civis especialistas, para operação assistida e assessoria.

5.5.3.3 As ligações com as agências deverão ser mantidas pelo Com D Ciber, e pelos órgãos regionais encarregados pela proteção e operação dos sistemas corporativos, como o Centro Integrado de Telemática do Exército (CITEx), os Centros de Telemática de Área (CTA) e os Centros de Telemática (CT).

5.5.4 Os elementos de ligação devem garantir que os representantes dos órgãos integrantes da estrutura de G Ciber tenham a clara compreensão da missão, das capacidades, das limitações e das necessidades de ligação das OM da F Ter vinculadas ao setor cibernético, além das considerações legais que envolvem sua missão. Os elementos de ligação com esses parceiros devem ter pleno entendimento sobre a natureza das relações de integração e dos tipos de suporte que esses órgãos podem oferecer.

5.5.5 Nas operações de cooperação e coordenação com agências, é dada ênfase maior a ações de proteção e de exploração cibernéticas.

5.6 OPERAÇÕES DE INFORMAÇÃO

5.6.1 A guerra cibernética contribui com as operações de informação como uma capacidade relacionada à informação (CRI). Assim, possui áreas de superposição com as Op Info, mas sem vínculo de subordinação. As CRI são aptidões requeridas para afetar a capacidade de oponentes ou potenciais adversários de orientar, obter, produzir e/ou difundir informações, em qualquer uma das três perspectivas da dimensão informacional (física, cognitiva ou lógica).

5.6.2 Para a G Ciber, os princípios fundamentais às Op Info de maior interesse são apresentados a seguir:

5.6.2.1 Direção e envolvimento pessoal do comandante – por esse princípio, o comandante tem conhecimento de todas as ações cibernéticas desencadeadas e pode empregar a G Ciber com técnicas adequadas para alcançar o estado final desejado (EFD).

5.6.2.2 Estreita coordenação – as tarefas devem ser coordenadas e sincronizadas com outras atividades operativas, de forma sinérgica, para evitar os efeitos colaterais pelo emprego de ações cibernéticas.

5.6.2.3 Acurada atividade de inteligência – as ações cibernéticas, quando alimentadas de informações confiáveis, têm resultados mais eficazes em prol do EFD.

5.6.2.4 Planejamento baseado em efeitos – as ações cibernéticas empregarão a técnica operacional de acordo com o efeito desejado: destruição, neutralização, inutilização, influência, dissimulação e negação da informação.

5.6.2.5 Envolvimento precoce e preparação antecipada – o planejamento das Op Info deve começar o mais cedo possível. De forma a contribuir para esse planejamento, as ações cibernéticas devem ser realizadas com a antecedência necessária, uma vez que seus resultados não são imediatos.

5.6.3 As ações cibernéticas a serem conduzidas em determinada operação devem ser mencionadas no apêndice de guerra cibernética ao anexo de operações de informação ao Pl/O Op da FTC.

REFERÊNCIAS

ALEMANHA. Federal Ministry of Defence. **Defence Aspects of Cybersecurity.** Berlin: Federal Ministry of Defence, 2012.

ASSUNÇÃO, M. F. A. **Segredos do Hacker Ético.** Florianópolis: Visual Books, 2010.

BRASIL. Exército. Centro de Defesa Cibernética. **A Defesa Cibernética como extensão do papel constitucional das Forças Armadas na Defesa Nacional.** Palestra institucional do CDCiber. Brasília, 2015.

BRASIL. Exército. Estado-Maior. **Bases para a transformação da Doutrina Militar Terrestre.** Brasília, DF: Estado-Maior do Exército, 2013.

BRASIL. Exército. Estado-Maior. **Glossário de Termos e Expressões para uso no Exército. C 20-1.** Brasília, DF: Estado-Maior do Exército, 2009.

BRASIL. Exército. Estado-Maior. I**nstruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro. EB10-IG-01.014.** Brasília, DF: Estado-Maior do Exército, 2014.

BRASIL. Exército. Estado-Maior. Instruções Gerais para as **Publicações Padronizadas do Exército. EB10-IG-01.002.** Brasília, DF: Estado-Maior do Exército, 2011.

BRASIL. Exército. Estado-Maior. **Manual de Campanha Abreviaturas, Símbolos e Convenções Cartográficas. C 21-30.** Brasília, DF: Estado-Maior do Exército, 2002.

BRASIL. Exército. Estado-Maior. **Manual de Campanha Comando e Controle. EB20-MC-10.205.** Brasília, DF: Estado-Maior do Exército, 2015.

BRASIL. Exército. Estado-Maior. **Manual de Campanha Força Terrestre Componente. EB20-MC-10.202.** Brasília, DF: Estado-Maior do Exército, 2014.

BRASIL. Exército. Estado-Maior. **Manual de Campanha Logística .EB20-MC-10.204.** Brasília, 2014.

BRASIL. Exército. Estado-Maior. **Manual de Campanha Operações em Ambiente Interagências. EB20-MC-10.201.** Brasília, DF: Estado-Maior do Exército, 2013.

BRASIL. Exército. Estado-Maior. **Manual de Campanha Processo de Planejamento e Condução das Operações Terrestres. EB20-MC-10.211.** Brasília, DF: Estado-Maior do Exército, 2014.

BRASIL. Exército. Estado-Maior. **Manual de Fundamentos Operações. EB20-MF-10.103.** 4. ed. Brasília, DF: Estado-Maior do Exército, 2014.

BRASIL. Exército. Estado-Maior. **Nota de Coordenação Doutrinária n. 02/ 2013. As Funções de Combate.** Brasília, DF: Estado-Maior do Exército, 2013.

BRASIL. Exército. **Relatório de Missão no Exterior . Conferência de Defesa Cibernética e Segurança de Redes (CDANS, Londres).** Brasília, DF: Estado-Maior do Exército, 2013.

BRASIL. Marinha. Estado-Maior da Armada. **Doutrina de Tecnologia da Informação da Marinha:** manual de Guerra Cibernética. EMA-416. Brasília, DF: Estado-Maior da Armada, 2013

BRASIL. Ministério da Defesa. **Concepção Operacional do Sistema Militar de Defesa Cibernética.** Brasília, DF: Ministério da Defesa, 2015.

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas. MD30-M-01.** Brasília, DF: Ministério da Defesa, 2011.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética. MD31-M-08.** Brasília, DF: Ministério da Defesa, 2014.

BRASIL. Ministério da Defesa. **Doutrina para o Sistema Militar de Comando e Controle. MD31-D-03.** Brasília, DF: Ministério da Defesa, 2014.

BRASIL. Ministério da Defesa. **Estrutura Militar de Defesa. MD35-D-01.** Brasília, 2010.

BRASIL. Ministério da Defesa. **Glossário das Forças Armadas. MD35-G-01.** Brasília, DF: Ministério da Defesa, 2007.

BRASIL. Ministério da Defesa. **Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas. MD33-M-02.** Brasília, DF: Ministério da Defesa, 2008.

BRASIL. Ministério da Defesa. **Manual de Operações de Paz.** Brasília, DF: Ministério da Defesa, 2013.

BRASIL. Ministério da Defesa. **Política Cibernética de Defesa.** Brasília, DF: Ministério da Defesa, 2012.

BRASIL. Ministério da Defesa. **Política de Segurança da Informação para o Sistema Militar de Comando e Controle.** Brasília, DF: Ministério da Defesa, 2014.

CARNEIRO, A. S. L. **Capacitação de Recursos Humanos no Exército Brasileiro para a Segurança Cibernética:** desenvolvimento de competências para a atuação em uma Equipe de Tratamento de Incidentes de Rede. Tese (Doutorado em Ciências Militares) – Escola de Comando e Estado-Maior do Exército. Rio de Janeiro, 2012.

DIÓGENES, Y. **Security + SYO 301.** Rio de Janeiro: Comptia, 2014.

DIÓGENES, Y. **Security + SYO 401.** Rio de Janeiro: Comptia, 2015.

ESPANHA. Centro Criptológico Nacional. **Guía de Seguridad.** Madrid, 2011.

ESTADOS UNIDOS. Army. Cyber **Electromagnetic Activities. FM 3-38.** Washington, DC: Army, 2014.

ESTADOS UNIDOS. Army. **The Army Universal Task List. FM 7-15.** Washington, DC: Army, 2012.

FRANÇA. Ministère de la Defense. **Cyberdéfense.** Paris: Ministère de la Defense, 2011.

GRAVES, K. **Official Certified Ethical Hacker:** review guide. Indianapolis: Wiley Publishing, 2007.

HARRIS, S. **CISSP:** exam guide. 6. ed. New York: McGraw Hill, 2013.

KLIMBURG, A. (Ed.). **National Cyber Security Framework Manual.**Tallin: NATO CDD COE Publications, 2012.

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. **Hackers Expostos 7.** Porto Alegre: Bookman, 2014.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de redes em ambientes corporativos.** São Paulo: Novatec Editora, 2007.

COMANDO DE OPERAÇÕES TERRESTRES
CENTRO DE DOUTRINA DO EXÉRCITO
Brasília, DF, 8 de junho de 2017
www.cdoutex.eb.mil.br